Guest Editorial

Sokratis Katsikas

Faculty of Pure and Applied Sciences,
Open University of Cyprus,
33 Giannou Kranidioti Ave., Latsia 2220, Cyprus
Email: sokratis.katsikas@ouc.ac.cy

and

Center for Cyber and Information Security,
Department of Information Security and Communication Technology,
Norwegian University of Science and Technology,
P.O. Box 191, Gjøvik N-2802, Norway
Email: sokratis.katsikas@ntnu.no

Vasilios Zorkadis

Hellenic Data Protection Authority,
Kifissias 1-3, Athens 11523, Greece
Email: zorkadis@dpa.gr

Biographical notes: Sokratis Katsikas is Professor and Rector of the Open University of Cyprus and Professor with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Norway. His research interests lie in the areas of information and communication systems security and of estimation theory and its applications. He has authored or co-authored more than 260 journal publications, book chapters and conference proceedings publications and he has participated in more than 60 funded national and international R&D projects in these areas. He is serving on the editorial board of several scientific journals, he has authored/edited 39 books and has served on/chaired the technical programme committee of more than 600 international scientific conferences.

Vasilios Zorkadis has been working as the Secretariat's Director of the Hellenic Data Protection Authority since 2004. He received a Diploma in Electrical Engineering from Aristotle University of Thessaloniki, Greece and holds a PhD on Computer Network Security from University of Karlsruhe, Germany. He is author of books on 'Cryptography', and 'Information Theory' and author or co-author of more than 60 journal and conference papers on security and privacy protection. He taught for almost 20 years in Greek universities courses on Information Theory, Information Security, Cryptography, Computer Networks and Digital Communications. He is a founding member and the current president of the "Hellenic Council for the Information Society".

ICT innovations such as Big Data, Internet of Things, Cloud Computing as well as Intelligent Systems employed in e-government services raise issues relating to Security, Privacy and Data Protection. Governments want to integrate more services and enhance participation, but they have to convince the users that they can be trusted. At the same time e-government services need to improve their efficiency and to do so they need to reengineer their back office processes, to support them with intelligent systems, but also improve openness, collaboration and citizen participation. This last point can be hugely enhanced by offering citizens participation in devolved decision making and e-voting facilities for elections. Such services are often quoted as being dependent on political will, but are the systems and services ready? Are they privacy-friendly and secure to withstand attacks and malicious or even terrorist activities in cyberspace? Are they trustworthy to be embraced by the citizens in a digital world that is moving fast and becoming more intelligent? And finally, where should be drawn the 'golden line' between anonymity and confidentiality, and accountability and certification?

These were the questions and the focus of the 7th occasion of the *International Conference on e-Democracy* that was held in Athens, the cradle of democracy, on December 14–15, 2017. This special issue contains extended and expanded versions of seven selected papers that were presented in the conference.

The first paper of the special issue, entitled 'The Interslavic language as a tool for supporting e-democracy in Central and Eastern Europe', by Merunka et al., explores the relation between the quality of information systems that support democracy and public administration with the language that these systems use. The authors give an overview of the pros and cons of various language options and describe the results of public research in the form of surveys, as well as their own practical experiences. The authors posit that language, e-democracy, and education form a triangle of three inseparable, interdependent entities, and they propose the use of Interslavic, a zonal constructed language in such information systems operating in the Slavic countries between Western Europe and Russia.

The next four papers of the special issue deal with issues related to privacy. The first among those, entitled 'Big data in political communication: implications for group privacy', by Mavriki and Karyda, addresses the implications for group privacy of adopting big data analytics technologies in the area of political marketing and communication. The authors argue that the use of such technologies in a political context can have severe implications for group privacy, including (political) targeting of particular groups and biased decision making based on group behaviour. Further, the authors show that threats to group privacy may have long term implications for society, especially with regard to the impact of populist movements.

In the same cluster, the paper entitled 'Transparency-enabling information systems: trust relations and privacy concerns in open governance' by Gritzalis et al. examines the value of transparency-enhancing information systems from a citizens' perspective. In particular, the authors explore the impact of openness on citizens' trust, the impact of privacy requirements and regulations on these systems, and the effect that these have on the attitude of citizens towards openness. 'Diavgeia', the national transparency system in Greece is used as a case study. Users of the system have been surveyed and the results demonstrate that the system is a well-established, reliable data source, and is regarded potentially trust-enhancing. However, personal privacy risks related to the system seem to concern even supporters of the 'right to know' principle.

Sideri et al., in the paper entitled 'Enhancing university students' privacy literacy through an educational intervention: a Greek case-study' address the privacy paradox in online social networks and explore the effects of a long-term University-based educational intervention for enhancing students' digital knowledge and skills on the students' ability to protect their privacy in online social networks. Their results indicate that such interventions can have significant impact on students' attitude and behaviour, increasing both privacy awareness and concerns. The paper concludes with some concrete recommendations on good practices regarding similar future educational interventions.

The last paper in the cluster, entitled 'Anonymity in social networks: the case of anonymous social media', by Chatzistefanou and Limniotis, investigates whether the underlying personal data processing in 'anonymous' social networks may suffice to result in tracking or identification of the users. The authors analyse five popular anonymous smart applications by monitoring the outgoing traffic of Android devices in real-time when using these applications. They examine which personal data are being processed by either the anonymous networks or third parties, e.g., library providers and assess whether the information provided to the users by means of the respective privacy policies is sufficient. The results raise concerns, as there is personal data processing in place even in such 'anonymous' applications; this in turn implies that the anonymity of the users cannot be guaranteed.

A prerequisite to the provision of secure and seamless transactions between citizens, businesses, and public agencies in Europe is the existence and use of electronic identification and trust services. The eIDAS regulation constitutes a legal framework for such services in Europe. The paper entitled 'Authenticated academic services through eIDAS', by Maliappis et al. presents the design and implementation of two academic eIDAS-based services, namely the Erasmus student mobility and the certificate issuance services. To this end, a microservice architecture has been deployed.

The last paper of the special issue, entitled 'Redefining freedom of speech in the digital environment from an EU law perspective' by Jougleux, turns our attention again to citizen rights and discusses the freedom of expression in the digital environment from an EU law perspective. After an analysis of the general legal regulation of online freedom of expression the author uses copyright law as a case study of how balancing of rights is applied by the courts, with reference to the mechanism of blocking orders. In the last part of the paper, three characteristics of online freedom of expression are addressed, namely the application between individuals, the intermediaries' protection and the principle of neutrality.